Testimony by Alexander Botting

Before the

United States House of Representatives
Homeland Security Committee
Cybersecurity & Infrastructure Protection and Transportation & Maritime Security Subcommittees

Hearing on the topic of

"Securing Global Communications: An Examination of Foreign Adversary Threats to Subsea Cable Infrastructure"

OPENING REMARKS

Chairman Gimenez, Chairman Ogles, Ranking Member McIver, and Ranking Member Swalwell, distinguished members of the Subcommittees, thank you for the invitation to appear before you today to discuss the critical issue of subsea cable infrastructure security.

My name is Alex Botting and I serve as Senior Director for Global Security & Technology Strategy at Venable LLP and as a Global Fellow at NYU's Wahba Institute for Strategic Competition. For the past decade, I've worked on issues at the intersection of digital technology, telecommunications and security – promoting policies that will make foundational digital technologies more secure.

Over the past two years, I've devoted considerable time to the issue of subsea cable security and recently authored a whitepaper on the topic entitled *Shoring Up Subsea Security*. My testimony incorporates the key findings and recommendations from that whitepaper.

If I could leave you with just two takeaways from today's hearing, they would be:

1. Redundancy is resilience. If cables are abundant and repairs are swift, the impact of any incident is limited. This, in turn, significantly reduces the incentive for our adversaries to engage in sabotage. Accordingly, we should pursue more efficient and transparent approvals processes for laying and repairing subsea cables, while of course maintaining high security standards.

2. Our investigations into disruptions to subsea cables are insufficient. Roughly 70% of subsea cable disruptions are caused by human activity. Yet, in almost all cases we fail to investigate negligence or malicious intent. If we believe that our adversaries may intend to engage in

sabotage, we must develop the means to distinguish between accidental and intentional disruption and proactively investigate human-induced disruptions.

The following testimony provides recommendations for the U.S. Government across three areas: enhancing the resilience of the global subsea cable ecosystem; ensuring the security of individual submarine cables against known threats; and implementing appropriate legal and institutional frameworks.

The implementation of some will be led by U.S. government agencies which fall outside of this Committee's jurisdiction. I'd like to draw your attention to two specific recommendations which the Department of Homeland Security (DHS) would be well-positioned to lead as a member of Team Telecom and the Sector Risk Management Agency for Communications, IT and Maritime Transportation.

- DHS should collaborate with industry and other U.S. government stakeholders to conduct a comprehensive mapping of the submarine cable supply chain to identify potential choke points or areas of reliance on untrusted vendors and ensure that appropriate risk mitigations are in place.
- DHS should manage a proactive two-way intelligence sharing mechanism with trusted cable developers and vendors to pre-empt potential attacks, and support the evidentiary body needed to prosecute criminal activity.

As we seek to insulate ourselves against threats from our adversaries, we should note that the continental United States is quite well-protected against a major subsea cable outage. We are served by almost 100 subsea cable landings, more than any other country. These cables land at diverse points on the East and West coasts, markedly reducing the risk that a single incident inhibits our access to the global internet. Moreover, in contrast to the Radio Access Network market, trusted vendors are the dominant players.

Because subsea cables are part of a globally connected ecosystem, and U.S. force projection depends upon deployments beyond our shores, it's critical that we work with international partners to promote the implementation of policy best practices, and enhance one another's understanding of the threat environment.

Subsea cables underpin the global internet and, in an era where critical infrastructure is increasingly networked, they are foundational to the operation of critical services upon which we rely every day. Given their criticality, we should not take today's security for granted. It is essential that we stay ahead of emerging security threats and resilient against incidents. Doing so will require robust multi-stakeholder and multi-country cooperation.

WHY SUBSEA CABLES ARE ESSENTIAL

There are few technologies more foundational to the modern economy than subsea cables. As of 2024, five and a half billion people had access to the global internet and the associated economic benefits. A network of 597 subsea fiber optic cables[i], largely operated by the private sector, enable them to do so by carrying more than 95% of intercontinental data traffic.[ii] Beyond use by individuals, subsea cables are essential to the operation of critical sectors including financial services, defense, and telecommunications.

Today the most advanced cables can transmit more than 350 terabits per second along the ocean floor, equivalent to "the entire digitized Library of Congress three times every second."[iii] This achievement is driven by investments in technological innovation and the global economy's insatiable demand for data, which has risen from roughly 100 gigabytes of traffic per day in 1992,[iv] to an estimated 495.89 million terabytes per day in 2025.[v]

With advanced-AI workloads introducing new demands for the movement of data, global demand will continue to grow significantly in the years ahead. There is no feasible pathway to meet this demand that does not include significant investment in subsea cable infrastructure.

The rapid deployment of Low Earth Orbit (LEO) satellites is an impressive technological feat, but as of 2024 the combined capacity of every SpaceX satellite was a little under 350 terabits per second.[vi] A single cutting-edge cable such as the "Grace Hopper", meanwhile, can transmit 352 terabits of data per second.[vii] As modern societies come to depend ever more on data and computing capabilities, the "cloud under the sea" is indispensable to the operation of a modern economy.

Given the critical function that they fulfill, submarine cables should be, and in many countries are, categorized as critical infrastructure themselves. This designation affords them additional attention from industry and government stakeholders to ensure their ongoing security and resilience.

THE THREAT ENVIRONMENT FOR SUBSEA CABLE INFRASTRUCTURE

Owing to the vast distances that they cover, subsea cables are inherently vulnerable to accidental damage, natural disasters, or malicious interference. Across the 597 cables in operation today, roughly 150-200 incidents impact their operations during a typical year, according to the International Cable Protection Committee (ICPC).[viii]

Recent disruptions to cables and rising geopolitical tensions have spurred governments to intensify scrutiny of submarine cable accidents. Public reporting that China has developed a cable-cutting device capable of severing highly fortified cables at a depth of 4,000 meters has amplified concerns.[ix] As has the discovery of "Project Harmony", a seabed sensor network

established by Russia.[x] Concerns have been amplified further by high-profile instances of cable disruptions in the Baltic Sea[xi] and the Taiwan Strait[xii], the latter of which saw more cable disruptions in January 2025 than in either 2023 or 2024.

In an era of deep mistrust, it is easy to overstate the extent of exploitation occurring today. Yet, while sabotage may occur, it is in all likelihood rare. According to ICPC, the vast majority of incidents – approximately 70% in any given year – are caused by physical damage from fishing activity or anchoring.[xiii] The remainder result from natural events (such as storms or earthquakes), abrasion, or internal system failures. These incidents are longstanding and typically well-managed.

Beyond cuts to subsea cables, there is a theoretical risk of data interception on a subsea cable. As noted on pages 12-13, at this time this is unlikely to be implemented in practice without detection. Nevertheless, while the risk of exploitation is low today, public and private sector stakeholders should continue to assess the capabilities of adversaries, informed by government intelligence where possible, and adjust their assessment of the risk accordingly.

Finally, there is the risk that untrusted vendors in subsea cable supply chains could compromise the confidentiality of data, or availability of networks. This issue parallels the challenges faced during the rollout of 5G communications when Chinese companies like Huawei and ZTE leveraged government subsidies to dominate the telecommunications market, especially in emerging economies.

China continues to lead in advanced optical communications research, producing 37.7% of the field's research compared to just 12.8% from the U.S., underscoring the urgency for democratic nations to restrict untrusted vendors from developing and controlling optical core network infrastructure.[xiv] Today, trusted vendors maintain a technological advantage and a leading market position, but we should not take this for granted.

PROMOTING RESILIENCE IN THE ECOSYSTEM

Cable Redundancy

Building redundancy into submarine cable routes is vital for the resilience and reliability of global communications. If cables are abundant and repairs are swift, cuts will have limited practical impact. This significantly reduces the incentive for our adversaries to engage in sabotage.

To enhance resilience, companies design networks such that each node connects to at least two others, allowing traffic rerouting. They also seek to ensure that the supply of capacity stays ahead of demand at both a local and global level. The building of new cables is resource intensive, however, often requiring hundreds of millions of dollars in investment.

Cumbersome and opaque permitting and licensing regimes add to expense and extend the timeline for deployments, discouraging investment. In the U.S., permitting timelines have stretched from under a year to over three years, involving up to eleven agencies with overlapping mandates for environmental, historical, and national security concerns. [xv] Moreover, national security reviews are often slow and can result in the denial of a landing license after years of investment, where government guidance earlier in the process could have redirected cable operators to more palatable routes or partners.

This lack of coordination, transparency, and predictability creates uncertainty, deters investors, and can even increase vulnerability through geographic clustering. Enhancing transparency with trusted private sector partners and streamlining permitting and licensing processes, while maintaining security standards, is thus critical to enhancing resilience.

In instances where laying additional subsea cables isn't commercially feasible, such as in remote islands, governments and development partners should explore alternative financing mechanisms or satellite-based alternatives to subsea cables to ensure resilience against single points of failure.

Recommendations

1. The U.S. Government should ensure that permit requirements for the installation and repair of submarine cables are transparent and establish clear timeframes for approvals that are as short as possible, without undermining security.
2. The U.S. Government should enhance clarity and predictability of rules, partners, and geographies that will factor into approvals decisions, and promote transparency between national security agencies and submarine cable developers about security risks.
3. The U.S. Government should establish and communicate clear security and resilience requirements which are aligned with international standards and harmonized with national security review processes.

Effective route planning

At a global level, route diversity is a common best practice as it allows data to reroute around damaged segments, reducing disruption and deterring sabotage. Within a given country's EEZ, however, governments and industry may decide between diversifying cable routes and landings or concentrating them in Cable Protection Zones (CPZs).[xvi]

While diversification minimizes the impact of an individual incident, it's not always feasible for countries with limited coastline, crowded marine environments, or facing hostile maritime disputes, such as the South China Sea. Where diversification isn't possible, Cable Protection Zones (CPZs) can safeguard concentrated routes by restricting anchoring and fishing. Governments must, however, enforce protection measures and penalize violations to reduce the risk that one event could damage multiple systems.

Ultimately, the U.S.'s current approach of diversifying cable routes and landings is the most appropriate for its circumstances.

Recommendations

4. The U.S. Government should foster commercial and regulatory conditions that support the development of diverse submarine cable landing sites and pathways, including streamlining permitting approvals processes.
5. The U.S. Government should establish regulatory frameworks that embed submarine cable considerations into marine spatial planning processes, ensuring early-stage coordination with submarine cable stakeholders during the planning and development of other marine activities.
6. The U.S. Government should coordinate with trusted international partners to harmonize (to the extent possible) licensing and permitting requirements.

Facilitating timely cable repairs

Fast, efficient repairs limit the disruption from security incidents, yet cabotage laws, permitting delays, customs fees, high costs, and limited repair vessels slow recovery efforts on many cables today. Although most systems can be repaired within two weeks, recent data show average repair times now go beyond that, owing to delays caused by permitting, weather, or backlogs.[xvii]

The imposition of cabotage requirements, which mandate the use of locally built and crewed vessels, is a problem at a global level. These rules increase costs, delay urgent repairs, and conflict with international law under UNCLOS, which affirms freedom to maintain cables in international and exclusive economic zones.[xviii]

Likewise, mandatory port calls and customs duties add unnecessary delays and costs. Streamlining entry procedures and eliminating taxes and tariffs on repair operations accelerates service restoration. Establishing free ports with bonded storage facilities further reduces friction, allowing secure, duty-free storage of repair materials until needed.

Recommendations:

7. The U.S. Government should actively engage with international partners to address barriers to cable repair, which not only impair local capacity but also undermine the resilience of the global ecosystem. This includes:

    7.1 Refraining from classifying submarine cable installation and repair activities as cabotage and from imposing cabotage or crewing restrictions on repair vessels.

    7.2 Eliminating port entry requirements for cable ships engaged in installation or repair operations.

7.3 Avoid imposing customs duties, taxes, and fees on submarine cable installation and repair activities, by enabling the establishment of Free Ports with bonded storage facilities at vessel base ports to facilitate deployment and expedite repairs.

Global repair ship capacity

The global fleet of repair ships is limited in size and distributed across the globe, which can cause delays in remote or high-traffic areas. Although most repair operations are handled by trusted entities, we do rely on a narrow vendor base that includes as least one untrusted vendor – China's S.B. Submarine Systems (SBSS) – which participates in repair efforts in the North Pacific region.[xix]

The U.S. established the Cable Security Fleet (CSF) in 2021, to ensure rapid response and repair capacity during emergencies. While this program strengthens U.S. capabilities, each new repair ship costs over $100 million, requiring a long-term commitment.[xx] Governments should ensure private sector involvement in developing public policy initiatives to boost repair, to ensure that they do not inadvertently reduce incentives for private industry to invest in and maintain commercial repair capacity.

Instead, the U.S. Department of Homeland Security should collaborate with industry to develop an emergency response capability, designed for targeted interventions in exceptional circumstances, such as major natural disasters or acts of sabotage.

Recommendations:

8. The U.S. Government should co-develop a strategy with industry for emergency cable repair capacity, to enable additional government resources to be deployed in the event of a widespread disruption to cables.
9. The U.S. Government should streamline regulatory frameworks to ensure efficient cable repair, while maintaining security and transparency. This includes improving permitting and liability regimes.

Secure and trusted supply chains

Resilience is dependent upon access to uninterrupted provision of the trusted components necessary for laying, repairing, and maintaining submarine cables. Today, global repair and installation capacity is concentrated among a few providers, leaving little room for expansion and creating potential chokepoints. Because no single country has enough repair demand to sustain its own market, operators rely on regional maintenance agreements to share ships and resources.

Within subsea cable infrastructure supply chains, potential market dominance by untrusted vendors, especially Chinese state-backed firms, poses a strategic risk. As seen during the 5G rollout with Huawei and ZTE, such control can enable authoritarian influence over global communications.

While trusted vendors lead the market today, China's leadership in optical communications research, producing nearly 38% of global output versus 13% from the U.S., underscores the need for the U.S. to invest in innovation, strengthen domestic R&D, and avoid dependency on Chinese vendors.[xxi] Collaboration between cable operators and governments to mitigate these risks is critical.

Recommendations:

10. DHS should collaborate with industry to conduct a comprehensive mapping of the submarine cable supply chain to identify potential choke points or areas of reliance on untrusted vendors and ensure that appropriate risk mitigations are in place.
11. The U.S. Government should maintain a published list of untrusted providers which will guide industry in the development of their supply chain partnerships.
12. The U.S. Government and trusted industry partners should cooperate on sharing risk and incident data to identify protection gaps, enhance resilience, and detect and prevent malicious activities by state and non-state actors.

ENHANCING THE SECURITY OF CABLE INFRASTRUCTURE

Submarine cables are engineered to withstand extreme underwater conditions, protected by multiple layers of insulation and armoring. While they rest along the seabed in deeper waters, they are typically buried 0.5-3 meters deep when at less than 1500 meters to protect against damage.[xxii] Despite these measures, cables remain vulnerable to natural, accidental, and intentional harm.

Events such as earthquakes, volcanic eruptions, tsunamis, and underwater landslides occasionally damage cables, though less frequently than human activity. The most prevalent cause of disruption, however, is human disruption caused by fishing and anchoring, which accounts for roughly 70% of cable breaks annually.[xxiii]

Several mitigations are available and are being utilized to address these risks, particularly those related to accidental and intentional human activities. The most obvious measure is armoring cables for tensile and impact resistance.

Beyond physical reinforcement, Automated Identification Systems (AIS) or Vessel Monitoring Systems (VMS) can be used to provide real-time alerts regarding vessel movements, which facilitates better cable protection.[xxiv] It also aids the investigation of incidents after they occur.

Recommendations:

13. Industry should continue to armor cables deployed shallower than 1500 meters.
14. The U.S. Government should ensure the use of AIS tracking devices by vessels is mandatory in national law and enforce its use in accordance with IMO regulations.
15. Governments should explore making the use of VMS tracking mandatory within their EEZ to enhance visibility of activity near submarine cables, and enforcement against negligent activities.

Physical Security of Landing Stations

Of the world's 1.5 million kilometers of submarine fiber-optic cables, all connect to land through roughly 1,400 Cable Landing Stations (CLS). These shoreline facilities link subsea cables to terrestrial infrastructure – such as fiber-optic networks and satellites – that carry data to users and data centers. Like other critical infrastructure, CLS facilities face risks from natural hazards such as hurricanes, wildfires, and earthquakes, as well as intentional threats from malicious actors. A 2017 U.S. government report identified landing stations as "the most accessible and impact-rich targets"[xxv] within global communications systems.

While internet traffic can often be rerouted through other terrestrial or subsea pathways, damage to a major CLS that connects multiple cables can still cause widespread outages.[xxvi] For this reason, network designers build redundancy by diversifying cable routes and landing points.

Protection of CLS sites is relatively comprehensive due to their fixed locations and clearer jurisdictional control. Standard safeguards include physical security measures—such as surveillance, access control, and intrusion detection—as well as resilience planning for energy supply and disaster impacts. Together, these practices form a mature framework for protecting critical coastal infrastructure that underpins global connectivity.

Recommendations:

16. The U.S. Government should work with industry to define clear security best practices for cable landing stations and work cooperatively to implement risk-based measures that enhance the overall resilience and security.

Interception of Data on Cables

Given the technical complexity of this type of espionage, the theoretical risk is unlikely to be implemented effectively at this time for three reasons: it requires enormous technical and financial resources, the sheer data volume makes useful extraction nearly impossible, and any physical interference will create detectable anomalies in the cable's performance.

Interfering with active cables post-deployment, however, is highly complex and limited to nation-states with advanced resources. There are reasonable concerns about Chinese-operated vessels like SBSS[xxvii] and research ships such as *Tan Suo Yi Hao*[xxviii] conducting suspicious activities near major cable routes. Yet much of the data that traverses networks today is encrypted. Even attempts to pursue a "harvest now, decrypt later"[xxix] strategy would require sufficient storage to retain up to 352 TBPS of data, overwhelming the resources of even the most well-resourced actors and creating a "needle in a haystack" problem. Moreover, any attempts to tamper with the cable undersea would likely create anomalies in the light passing through the cable, which would be captured by the modems.

To mitigate future threats, data owners should implement strong encryption in transit and plan migration to post-quantum cryptography. Ultimately, however, given the vast resources required and without a clear path to generating usable information, the risk associated with cable 'tapping' remains very low and the efforts of adversarial nation states are likely to be directed toward more accessible targets.

Vulnerabilities could, however, be introduced during manufacturing or storage. Cable components kept in depots, such as China's Wujing Depot, may face higher tampering risks due to weaker security controls. While there is currently limited public evidence of exploitation, the long-term storage of components in jurisdictions of strategic concern warrants continued vigilance and mitigation of risks.

<u>Recommendations:</u>

17. Industry owners of data should continue to implement comprehensive data risk mitigation frameworks including, where feasible, encrypting data in transit.
18. The U.S. Government and industry owners of data should ensure timely transition to quantum-resistant algorithms when encrypting sensitive data.
19. DHS should work with industry to map potential supply chain risks, to include those to the repair supply chain.

Emerging Detection Capabilities

One emerging technology – fiber sensing – can also play a role in improving real-time incident detection. Fiber sensing leverages the optical transmission technology used by modern cables to

send information between endpoints. The oscillation direction of the electric field, known as the State of Polarization (SOP), changes as the light propagates. The SOP is sensitive to external stimuli, such as the pressure and physical movements experienced by the fiber, enabling fiber sensing technologies integrated into modems to monitor and detect variations to the SOP.[xxx]

By analyzing these changes, operators can gain valuable insights into the physical movements or disturbances affecting the cable, enabling real-time detection of tampering or damage. Beyond detecting damage to cables after they have gone offline, fiber sensing can provide insights into underwater activity in the vicinity of submarine cables. This could improve investigations, support attribution of incidents, and increase accountability, thereby enhancing deterrence.

Additionally, fiber sensing can serve as an early warning system for natural hazards. For example, changes in the SOP of a particular submarine cable caused by an underwater earthquake could provide information to early warnings of tsunamis, allowing governments to mitigate harms to populated areas.

While fiber sensing may enhance situational awareness and cable protection, however, its deployment raises important legal considerations. Adding fiber sensing to a cable may reclassify it from a purely telecommunications cable to a measurement device. To enable the widespread use of fiber sensing on cables crossing such jurisdictions, further clarification of UNCLOS provisions will be necessary to ensure continued compliance with international law.

Recommendations:

20. The U.S. Government and industry should continue to invest in research and development (R&D) to advance fiber sensing capabilities and establish clear guidance on the approvals process for, and use of, fiber sensing solutions.

21. The U.S. Government and industry should explore potential information sharing agreements to leverage real-time data regarding imminent natural disasters.

IMPLEMENTING LEGAL & INSTITUTIONAL FRAMEWORKS

Domestic Legal Frameworks

Legal and institutional frameworks play a critical role in reinforcing risk mitigation and deterrence. If designed effectively, they will catalyze security and resilience efforts by promoting awareness of risks, enhancing multi-stakeholder coordination, reducing instances of unintentional disruption, and adequately deterring acts of aggression.

Governments can play a constructive role firstly by enhancing transparency around national security priorities. For example, publishing clear guidance on high-risk countries, prohibited

equipment, and entities and countries of concern would help infrastructure operators make informed decisions.

Secondly, by implementing national obligations under 1884 and UNCLOS. Article II of the former states that it's "a punishable offence to break or injure a submarine cable, willfully or by culpable negligence, in such a manner as might interrupt or obstruct telegraphic communication."[xxxi] Article 113 of UNCLOS, meanwhile, requires countries to adopt laws to punish people or ships under its jurisdiction for damaging or breaking submarine cables on the high seas, whether "done willfully or through culpable negligence."[xxxii] Yet while on the surface this provides a robust enforcement framework, in reality it is enforced sporadically.

Thirdly, by enforcing IMO-required use of Automatic Identification Systems (AIS). AIS is required to be fitted on most large ships. Yet according to a recent study, enforcement is poor and "sanctions are not severe enough to act as deterrents."[xxxiii] Many vessels deactivate AIS to evade detection while illegally fishing in protected areas or to avoid revealing lucrative fishing areas to competitors.[xxxiv]

Finally, governments should ensure coordinated use of the territorial seabed. This can be done by mandating educational programs for maritime employees via local marine and fishing authorities, to ensure they are aware of key cable pathways, charting requirements, and measures to avoid accidental disruption.

Where fishing vessels are negligent in applying these measures, penalties should be enforced, even in cases of accidental disruption, to incentivize compliance. Due to the inherently cross border nature of this infrastructure, the U.S. should also promote their implementation by foreign governments.

Recommendations:

22. The U.S. Government should implement national obligations under 1884 and UNCLOS, where applicable.
23. The U.S. Government should ensure IMO-required use of Automatic Identification System (AIS) tracking.
24. The U.S. Government should ensure that charting authorities update nautical charts regularly; ensure implementation of the amended IHO Resolution 4/1967; and mandate educational programs for employees of maritime vessels.
25. The U.S. Government should establish and rigorously enforce penalties for the disruption of cables through negligence and encourage international partners to do the same.

International Collaboration

Effective deterrence necessitates the ability to monitor, intercept, and penalize vessels that may cause disruption within the territorial sea. The cable ecosystem covers such vast territory, however, that it would require an unfeasible number of resources for countries to patrol the high seas individually.

The U.S. Government should work with international partners, leverage existing security mechanisms such as NATO or the Quad, to establish a multilateral mechanism for conducting patrols, focused on high-risk areas. These include regions that are experiencing acute geopolitical instability (e.g. Baltic Sea), have cables that are more physically exposed (e.g. Red Sea), or are key fulcrums for the global ecosystem (e.g. Straits of Malacca).

Supporting these efforts, governments should establish or expand mechanisms for intelligence-sharing with trusted partners to pre-empt potential attacks, adapt patrol activities accordingly, and support the evidentiary body needed to convict saboteurs. While the private sector has proven itself adept at ensuring continuity of service during past outages, only governments can conduct the kind of operational activities needed to deter acts of international negligence or aggression.

Beyond operational collaboration, there are critical gaps in the existing international legal architecture for submarine cables. Even if likeminded countries enforce their obligations under 1884 and UNCLOS at a domestic level, state actors can opt not to impose penalties on ships bearing their flag that engage in sabotage on the High Seas. As recent disruptions in the Baltic Sea and Taiwan Strait have demonstrated, existing legal frameworks in many countries make it highly challenging to intercept, investigate, or prosecute security incidents, even where governments suspect intentional foul play.[xxxv] Whether these incidents are deemed to be accidental or intentional acts of sabotage, our inability to address acts of sabotage if and when they occur inhibits our ability to deter such behavior.

Recommendations:

26. The U.S. Government should leverage existing security cooperation agreements to conduct patrols in high-risk areas and share intelligence about potential threats.
27. DHS should manage a proactive two-way intelligence sharing mechanism with trusted cable developers and vendors to pre-empt potential attacks, and support the evidentiary body needed to prosecute criminal activity.

Multi-Stakeholder Coordination

Government and industry have a shared interest in promoting the security and resilience of submarine cable infrastructure, yet mechanisms for public-private coordination are limited. To remedy this, governments should take steps to formalize their private sector engagement. These

efforts should initially focus on: establishing a Single Point of Contact (SPOC) for private sector engagement; establishing two-way threat intelligence sharing with private stakeholders; and enhancing transparency around trusted vendors.

In most governments, multiple agencies have responsibility for some aspect of submarine cable resilience. Their remit may cut across environmental, commercial, or security considerations and their authorities may encompass new cable approvals, repair activities, or critical infrastructure protection. Governments can reduce inefficiencies, while meeting desired security outcomes, by appointing a SPOC responsible for engaging companies as they navigate regulatory processes. Their role would not prevent direct engagement with individual agencies. Rather, this office would serve as the primary external liaison to private entities and internally drive maximum efficiency and transparency of the process.

The important role of private companies in deploying, maintaining, and securing these assets also necessitates multi-stakeholder threat intelligence sharing. This enables public and private organizations to benefit from information, analysis, and context that they would not be privy to individually and provides an early warning system against potential threats. Beyond direct information about tactics, techniques and indicators of compromise, this creates a common understanding of the threat environment and what steps need to be taken to mitigate risks.

Untrusted vendors have been successful in winning contracts for subsea cable infrastructure. While this is less acute than in Radio Access Networks, organizations like HMN continue to leverage significant Chinese government subsidies to undercut bids from competitors by up to a third.[xxxvi] While matching China's bids dollar-for-dollar is not a feasible long-term solution, likeminded governments can reduce the strategic advantage of untrusted vendors by publishing clear guidance on high-risk equipment, entities of concern, and trusted suppliers. This transparency would help infrastructure operators make informed procurement decisions early in the planning process and ensure alignment with national security objectives. Such guidance can also deter the use of untrusted vendors by signaling potential risks, while supporting trusted vendors in producing competitive, security-enhancing bids.

Recommendations:

28. The U.S. Government should serve as a single point of contact to centralize information and serve as an initial liaison for government agencies, and private parties regarding existing and planned submarine cables.

29. The U.S. Government should publish clear guidance on high-risk equipment, entities and countries of concern, and trusted suppliers.

30. The U.S. Government should establish formal 1.5 track dialogues with trusted industry partners through existing regional and security groupings, such as the Quad and NATO, to support aligned approaches to submarine cable security and resilience.

[i] TeleGeography, Submarine Cable Map 2025, https://submarine-cable-map-2025.telegeography.com/.
[ii] TeleGeography, "Submarine Cable Frequently Asked Questions," (last accessed Nov. 17, 2025). www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions.
[iii] Chris Ciauri, "The Dunant subsea cable, connecting the US and mainland Europe, is ready for service," Google, Feb.3, 2021, cloud.google.com/blog/products/infrastructure/googles-dunant-subsea-cable-is-now-ready-for-service.
[iv] UNCTAD, *Global efforts needed to spread digital economy benefits https://unctad.org/news/global-efforts-needed-spread-digital-economy-benefits-un-report-says*
[v] https://www.statista.com/statistics/871513/worldwide-data-created/
[vi] Universe Space Tech, "SpaceX presents Starlink V3 satellites with 1 Tbps speeds," Jan 7, 2025, https://universemagazine.com/en/spacex-presents-starlink-v3-satellites-with-1-tbps-speeds/?srsltid=AfmBOor-h6nkfdYkNrl-hH5gyGg_XH6PFBeM00ZrWa_FyOtc4ecNdVBE.
[vii] Federal Communications Commission, Report No. SCL-00352 Actions Taken Under Cable Landing License Act, Jan. 14, 2022, https://docs.fcc.gov/public/attachments/DA-22-44A1_Rcd.pdf#:~:text=Cable%20Design%20and%20Capacity:%20Grace%20Hopper%20will,system%20design%20capacity%20of%20approximately%20352%20Tbps..
[viii] International Cable Protection Committee (ICPC), Media Enquiries & Frequently Asked Question, May 16, 2025, https://www.iscpc.org/news/media-enquiries/.
[ix] The Diplomat, "China's new deep-sea cutting tool exposes vulnerability of undersea cables," April 16, 2025, https://thediplomat.com/2025/04/chinas-new-deep-sea-cutting-tool-exposes-vulnerability-of-undersea-cables/.
[x] International Consortium of Investigative Journalists, "Russia secretly acquired Western technology to protect its nuclear submarine fleet," Oct. 23, 2025, https://www.icij.org/investigations/russia-archive/russia-secretly-acquired-western-technology-to-protect-its-nuclear-submarine-fleet/.
[xi] Associated Press, "Sweden seizes vessel suspected of 'sabotage' after undersea data cable rupture in Baltic Sea," Jan. 27, 2025, https://apnews.com/article/latvia-denmark-underwater-cable-damage-investigation-63da5ef0d577bca12bbe118d527d3a14.
[xii] ABC News, "Taiwan detains China-linked cargo ship after undersea cable disconnected," Feb. 25, 2025, https://www.abc.net.au/news/2025-02-25/taiwan-detains-china-linked-ship-after-undersea-cable-incident/104981932.
[xiii] ICPC, "Charting submarine cables is critical for maritime safety & infrastructure protection," June 25, 2025, https://www.iscpc.org/publications/icpc-viewpoints/charting-submarine-cables-is-critical-for-maritime-safety-and-infrastructure-protection/.
[xiv] Australian Strategic Policy Institute (ASPI), Critical Technology Tracker, March 1, 2023, https://www.aspi.org.au/report/critical-technology-tracker/#6a5a9bb3-c58e-4909-85f4-78bd875c0a80-link.
[xv] Department of Homeland Security (DHS), Priorities for DHS Engagement on Subsea Cable Security & Resilience, Dec. 18, 2024, www.dhs.gov/publication/priorities-dhs-engagement-subsea-cable-security-resilience.
[xvi] International Cable Protection Committee, Government Best Practices for Protecting and Promoting Resilience of Submarine Telecommunications Cables Version 1.2, (last accessed Nov. 17, 2025), pg. 3, https://www.iscpc.org/documents/?id=3733.
[xvii] Recorded Future, Submarine Cables Face Increasing Threats Amid Geopolitical Tensions and Limited Repair Capacity, July 17, 2025, https://assets.recordedfuture.com/insikt-report-pdfs/2025/ta-2025-0717.pdf.
[xviii] ICPC, Government Best Practices, pg. 9
[xix] The Wall Street Journal, "U.S. Fears Undersea Cables are Vulnerable to Espionage from Chinese Repair Ships," May 19, 2024, https://www.wsj.com/politics/national-security/china-internet-cables-repair-ships-93fd6320?gaa_at=eafs&gaa_n=AWEtsqfyEGd0IiscfyyxW9hIWjo81A0KIhm6vclhvq9qX5Dqz5-zFdPBaDY037Uqm0Y%3D&gaa_ts=691b909c&gaa_sig=pdns4KMa_RE6jXl2cxwWTF-glzZzsrrZRQAdpCfsf6n2ZsYAsMqHUR5gu_R7fatAnf8Qg4vv_GmY-H4O3q3gtw%3D%3D.
[xx] Center for Strategic & International Studies (CSIS), Safeguarding Subsea Cables: Protecting Cyber Infrastructure amid Great Power Competition, August 2024, https://www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition.
[xxi] Australian Strategic Policy Institute (ASPI), Critical Technology Tracker, March 1, 2023, https://www.aspi.org.au/report/critical-technology-tracker/#6a5a9bb3-c58e-4909-85f4-78bd875c0a80-link.
[xxii] ICPC, Government Best Practices, pg. 2

[xxiii] ICPC, Government Best Practices, pg. 1
[xxiv] ICPC, Government Best Practices, pg. 2
[xxv] CRS, *Protection of Undersea Telecommunication Cables*, pg. 6.
[xxvi] Data Center Dynamics, "What is a cable landing station?"
[xxvii] Daniel Runde et. al., *Safeguarding Subsea Cables: Protecting Cyber Infrastructure amid Great Power Competition*, CSIS, Aug. 2024, pg. 4., www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition.
[xxviii] Samantha Dick and Stephen Dziedzic, "Dutton says Chinese research ship is collecting intelligence, mapping undersea cables," *ABC News,* Mar. 31, 2025, www.abc.net.au/news/2025-04-01/dutton-says-chinese-research-ship-mapping-undersea-cables/105122068.
[xxix] K. F. Hasan *et al*., *A Framework for Migrating to Post-Quantum Cryptography: Security Dependency Analysis and Case Studies,* IEEE Access, Feb. 16, 2024, pg. 23431
[xxx] Brian Lavallee, "Detecting Undersea Earthquakes with Cross-Industry Collaboration," *Ciena*, Feb. 22, 2024, https://www.ciena.com/insights/articles/2022/detecting-undersea-earthquakes-with-cross-industry-collaboration
[xxxi] *1884 Convention for the Protection of Submarine Telegraph Cables*, Mar. 14, 1884, p. 2, https://cil.nus.edu.sg/wp-content/uploads/2019/02/1884-Convention-for-the-Protection-of-Submarine-Telegraph - Cables-1.pdf
[xxxii] UN, *Convention on the Law of the Sea*, pg. 64
[xxxiii] Priyal Bunwaree, *The Illegality of Fishing Vessels 'Going Dark' and Methods of Deterrence*, Cambridge University Press, Jan. 11, 2023, pg. 191
[xxxiv] Oceana, "Avoiding Detection Global Case Studies."
[xxxv] Miranda Bryant, "Sweden says China denied request for prosecutors to board ship linked to severed cables," The *Guardian*, Dec. 23, 2024
[xxxvi] Joe Brock, "US and China wage war beneath the waves - over internet cables," *Reuters*, Mar. 24, 2023, https://www.reuters.com/investigates/special-report/us-china-tech-cables/